ADAMS ML080650740

U.S. Nuclear Regulatory Commission

Privacy Impact Assessment

(*Designed to collect the information necessary to make relevant determinations regarding the applicability of the Privacy Act, the Paperwork Reduction Act information collections requirements, and record management requirements.)*

for the

Individual Action Tracking System (IATS)

Date: February 20, 2008

A. GENERAL SYSTEM INFORMATION

1. Provide brief description of the system:

   The Individual Action Tracking System (IATS) tracks cases of individuals involved in NRC-licensed activities who have been subject to NRC enforcement actions.

2. What agency function does it support?

   IATS supports the Office of Enforcement (OE) in their ability to track and trend enforcement actions taken against individuals.

3. Describe any modules or subsystems, where relevant, and their functions.

   N/A

4. Points of Contact:

Project Manager	Office/Division/Branch	Telephone
June Cai	Office of Enforcement	301-415-5192
Business Project Manager	Office/Division/Branch	Telephone
June Cai	Office of Enforcement	301-415-5192
Executive Sponsor	Office/Division/Branch	Telephone
Cynthia Carpenter	Office of Enforcement	301-415-2741

5. Does this Privacy Impact Assessment (PIA) support a proposed new system or a proposed modification to an existing system?

a. ___ New System ___ Modify Existing System __X__ Other (Explain)

PIA supports a system that has been in existence for several years.

b. If modifying an existing system, has a PIA been prepared before?

(1) If yes, provide the date approved and ADAMS accession number.

B. INFORMATION COLLECTED AND MAINTAINED

(These questions are intended to define the scope of the information requested as well as the reasons for its collection. Section 1 should be completed only if information is being collected about individuals. Section 2 should be completed for information being collected that is not about individuals.)

1. INFORMATION ABOUT INDIVIDUALS

a. Does this system maintain information about individuals?

Yes

(1) If yes, what group(s) of individuals (e.g., Federal employees, Federal contractors, licensees, general public) is the information about?

General Public – who work at or for an NRC licensee; including licensee contractors.

b. What information is being maintained in the system about individuals (describe in detail)?

The individual's first and last name.

c. Is the information being collected from the subject individuals?

Yes

(1) If yes, what information is being collected from the individuals?

Individual's name is taken as a sworn testimony during an Office of Investigations (OI) investigation.

d. Will the information be collected from 10 or more individuals who are **not** Federal employees?

Yes.

(1) If yes, does the information collection have OMB approval?

No

(a) If yes, indicate the OMB approval number:

e. Is the information being collected from internal files, databases, or systems?

Internal files

(1) If yes, identify the files/databases/systems and the information being collected.

OI investigation report and enforcement action

f. Is the information being collected from external sources(s)?

No

(1) If yes, what are the source(s) and what type of information is being collected?

g. How will this information be verified as current, accurate, and complete?

Information is taken as sworn testimony by the individual during an OI investigation. Individual's name is entered into the system manually by an enforcement specialist.

h. How will the information be collected (e.g. form, data transfer)?

Information collected by OI recording of testimony and field notes. Data provided to OE through issuance of the OI investigation report.

i. What legal authority authorizes the collection of this information?

Atomic Energy Act of 1954. Also 42 U.S.C 2113, 2114, 2231; 42 U.S.C. 2167, as amended; 42 U.S.C. 2201(I), as amended; and 42 U.S.C. 2282, as amended; 10 CFR 30.10, 40.10, 50.5, 60.11, 61.9b, 70.10, 72.12, and 110.7b.

j. What is the purpose for collecting this information?

To allow the office to track and trend actions taken against individuals.

2. **INFORMATION NOT ABOUT INDIVIDUALS**

a. What type of information will be maintained in this system (describe in detail)?

A unique system tracking number, the type of sanction issued against the individual (violation, letter, order); violation type including a brief description of the violation committed; licensee type and location, and whether it was a licensed individual or official.

b. What is the source of this information? Will it come from internal agency sources and/or external sources? Explain in detail.

Internal source. Letters/sanctions issued by OE after completion of enforcement process.

c. What is the purpose for collecting this information?

Track and trend sanctions against individuals.

C. USES OF SYSTEM AND INFORMATION

(These questions will identify the use of the information and the accuracy of the data being used.)

1. Describe all uses made of the information.

   Track sanctions taken against individuals, and trend individual enforcement actions.

2. Is the use of the information both relevant and necessary for the purpose for which the system is designed?

   Yes

3. Who will ensure the proper use of the information?

   OE specialists

4. Are the data elements described in detail and documented?

   No

   a. If yes, what is the name of the document that contains this information and where is it located?

5. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?

   No

a. If yes, how will aggregated data be maintained, filed, and utilized?

b. How will aggregated data be validated for relevance and accuracy?

c. If data are consolidated, what *controls* protect it from unauthorized access, use, or modification?

6. How will the information be *retrieved* from the system (be specific)?

By individual's name or unique tracking number

7. Will this system provide the capability to identify, locate, and monitor (e.g., track, observe) individuals?

No

a. If yes, explain.

(1) What controls will be used to prevent unauthorized monitoring?

8. Describe the report(s) that will be produced from this system.

- Current restricted individual list.
- Banned individual list.
- Types of violations/orders issued.
- Licensed vs. non-licensed individual list
- Actions taken since a specific period in time.

a. What are the reports used for?

Identify if individual previously committed a violation, and trending.

b. Who has access to these reports?

OE specialists

D. RECORDS RETENTION AND DISPOSAL

*(These questions are intended to establish whether the information contained in this system has been scheduled, or if a determination has been made that a general record schedule can be applied to the information contained in this system. Reference NUREG-0910, "*NRC Comprehensive Records Disposition Schedule*.")*

1. Has a retention schedule for this system been approved by the National Archives and Records Administration (NARA)?

Yes

a. If yes, list the disposition schedule.

Case files are permanent records and are transferred to NARA with related indexes when 20 years old in accordance with NARA approved schedule N1-431-00-05, Item 3a(1) and 3.a(4). All other enforcement actions and violations are destroyed 10 years after the actions are cut off, in accordance with NARA approved schedule N1-431-00-05, Item 3.b(1) and 3.b.(4).

2. Is there a General Records Schedule (GRS) that applies to information in this system?

a. If yes, list the disposition schedule.

3. If you answered no to questions 1 and 2, complete NRC Form 637, NRC Electronic Information System Records Scheduling Survey, and submit it with this PIA.

E. ACCESS TO DATA

1. INTERNAL ACCESS

a. What organizations (offices) will have access to the information in the system?

OE

(1) For what purpose?

Identify if an individual had previously committed a violation of NRC requirements.

(2) Will access be limited?

Yes

b. Will other systems share or have access to information in the system?

No.

c. How will information be transmitted or disclosed?

N/A

d. What controls will prevent the misuse (e.g., unauthorized browsing) of information by those having access?

Access on the internal G-drive which is password protected.

e. Are criteria, procedures, controls, and responsibilities regarding access documented?

(1) If yes, where?

2. **EXTERNAL ACCESS**

a. Will external agencies/organizations/public share or have access to the information in this system?

No access to the database; however, the sanction against the individual is made pubic on the NRC external Web site at the time the violation is issued to the individual.

(1) If yes, who.

b. What information will be shared/disclosed and for what purpose?

If a violation is committed by the individual, the individuals' name, identifier (IA number) and the sanction are listed on the NRC public Web site for a period of time to inform licensees of actions taken against individuals (i.e., banning from working at licensed facilities).

c. How will this information be transmitted or disclosed?

Information posted on NRC public Web site.

F. TECHNICAL ACCESS AND SECURITY

1. Describe security controls used to limit access to the system (e.g., passwords). Explain.

On internal G-drive (not NRC mainframe) limited to OE personnel, and system is password protected.

2. Will the system be accessed or operated at more than one location (site)?

No, but Enforcement specialists who have citrix could access the database from their home since they would have access to the G-drive.

a. If yes, how will consistent use be maintained at all sites?

3. Which user group(s) (e.g., system administrators, project manager, etc.) has access to the system?

   All OE specialists

4. Will a record of their access to the system be captured?

   No

   a. If yes, what will be collected?

5. Will contractors have access to the system?

   No

   a. If yes, for what purpose?

      - Ensure that the following Federal Acquisition Regulation (FAR) clauses are referenced in all contracts/agreements/purchase order where a contractor has access to a Privacy Act system of records to ensure that the wording of the agency contracts/agreements/purchase order make the provisions of the Privacy Act binding on the contractor and his or her employees:

        - 52.224-1 Privacy Act Notification.

        - 52.224-2 Privacy Act.

6. What auditing measures and technical safeguards are in place to prevent misuse of data?

   None

7. Are the data secured in accordance with FISMA requirements?

   No, system is off the shelf Microsoft software “Access”

   a. If yes, when was Certification and Accreditation last completed?

PRIVACY IMPACT ASSESSMENT REVIEW/APPROVAL
(For Use by OIS/IRSD/RFPSB Staff)

System Name: Individual Action Tracking System (IATS)

Submitting Office: Office of Enforcement

A. PRIVACY ACT APPLICABILITY REVIEW

___ Privacy Act is not applicable.

_X_ Privacy Act is applicable.

___ Privacy Act is applicable. Creates a new system of records. FOIA/PA Team will take the lead to prepare the system notice.

___ Privacy Act is applicable. Currently covered under System of Records, NRC- . Modification to the system notice is required. FOIA/PA Team will take the lead to prepare the following changes:

Comments:

The IATS is currently maintained as part of NRC's Privacy Act system of records NRC-3, "Enforcement Actions Against Individuals," therefore the information contained in the system is afforded the protections of the Privacy Act.

Reviewer's Name	Title	Date
Sandra S. Northern	Privacy Program Officer	March 13, 2008

B. INFORMATION COLLECTION APPLICABILITY DETERMINATION

_X_ No OMB clearance is needed.

___ OMB clearance is needed.

___ Currently has OMB Clearance. Clearance No._____

Comments:

The information collected and then maintained in this system is exempt from the Paperwork Reduction Act (PRA). Specifically, 44 U.S.C. 3518(c) defines certain purposes for which collection of information are exempt from all requirements of the PRA. This section outlines where an administrative action or investigation involving an agency against specific individuals or entities is exempt.

Reviewer's Name	Title	Date
Gregory Trussell	Team Leader- Information Collections	March 6, 2008

C. RECORDS RETENTION AND DISPOSAL SCHEDULE DETERMINATION

___ No record schedule required.

___ Additional information is needed to complete assessment.

___ Needs to be scheduled.

_X_ Existing records retention and disposition schedule covers the system - no modifications needed.

___ Records retention and disposition schedule must be modified to reflect the following:

Comments:

Records contained in the system are covered under NUREG-0910, page 2.10.8, NARA Schedule N1-431-00-5 Item 3.b(1)(c).

Reviewer's Name	Title	Date
Tracy L. Clark	Records Management Analyst	03/10/08

D. BRANCH CHIEF REVIEW AND CONCURRENCE

___ This IT system **does not** collect, maintain, or disseminate information in identifiable form from or about members of the public.

_X_ This IT system **does** collect, maintain, or disseminate information in identifiable form from or about members of the public.

I concur in the Privacy Act, Information Collections, and Records Management reviews:

/RAN/ Date: **03/13/2008**

Russell A. Nichols, Acting Chief
Records and FOIA/Privacy Services Branch
Information and Records Services Division
Office of Information Services

TRANSMITTAL OF PRIVACY IMPACT ASSESSMENT/
PRIVACY IMPACT ASSESSMENT REVIEW RESULTS

TO: **Cynthia Carpenter, Director, Office of Enforcement**	
Name of System: **Individual Action Tracking System (IATS)**	
Date RFPSB received PIA for review: March 3, 2008	Date RFPSB completed PIA review: March 13, 2008
Noted Issues: Part of NRC's Privacy Act system of records NRC-3, "Enforcement Actions Against Individuals." No information collection issues. Records disposition schedule: NUREG-0910, page 2.10.8, NARA Schedule N1-431-00-5 Item 3.b(1)(c).	
Russell A. Nichols, Acting Chief Records and FOIA/Privacy Services Branch Office of Information Services	Signature/Date: ***/RAN/*** **03/13/2008**
Copies of this PIA will be provided to: *James C. Corbett, Director* *Business Process Improvement and Applications Division* *Office of Information Services* *Paul Ricketts* *Senior IT Security Officer (SITSO)* *FISMA Compliance and Oversight Team* *Computer Security Office*	